QUALYS®

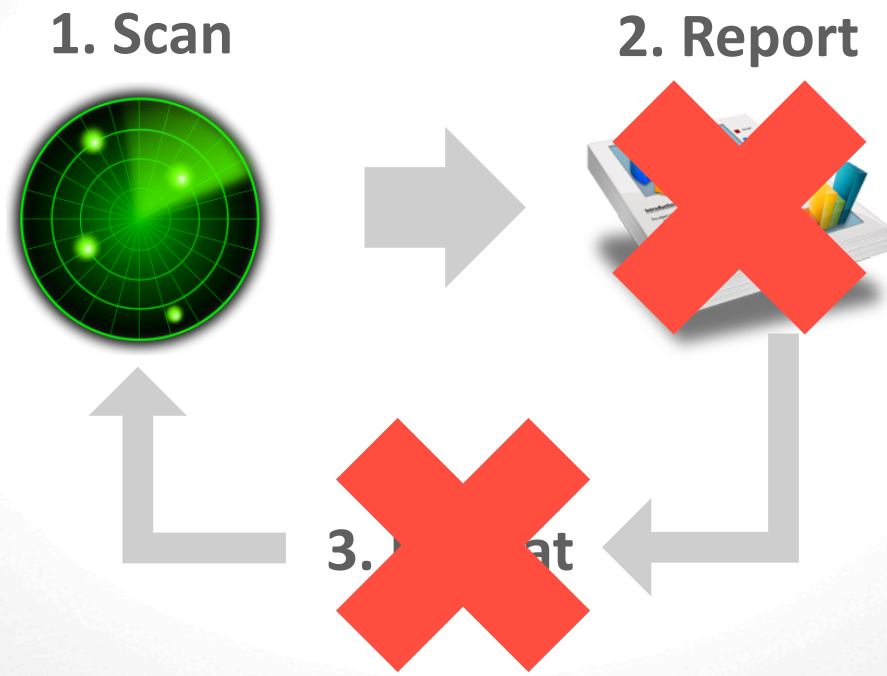
CONTINUOUS SECURITY

Continuous Monitoring
A New Approach to Security

Sean Molloy
Chief Architect

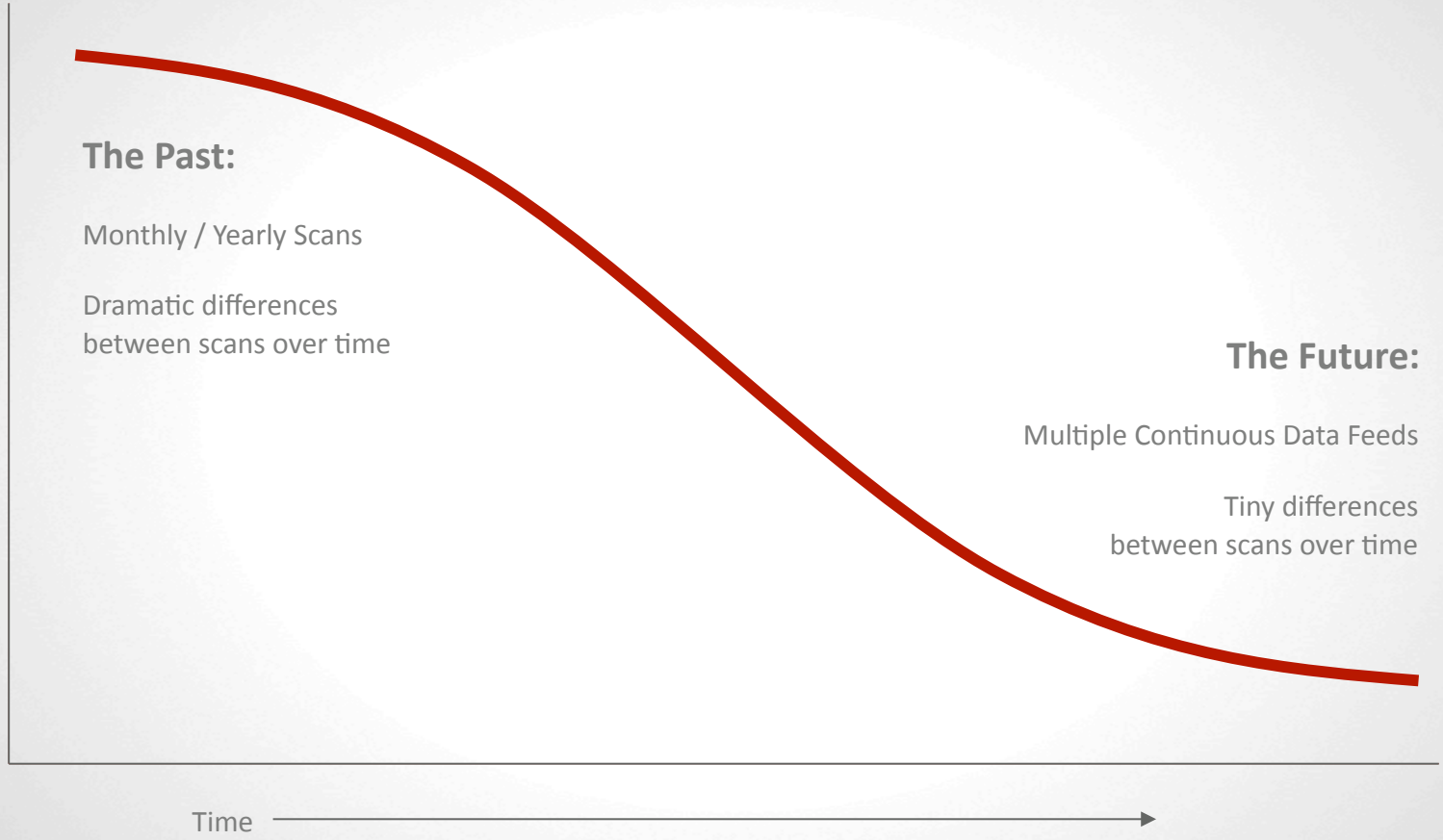
Historically, Vulnerability Management was all about **listing** and **reporting** your vulnerabilities.

The Simple Iteration



QUALYS®

Repetitive reporting doesn’t scale.


The Past:
Monthly / Yearly Scans
Dramatic differences between scans over time
The Future:
Multiple Continuous Data Feeds
Tiny differences between scans over time
Time

QUALYS®

Over the last year, **Qualys** has been laying the **foundation** for a **new breed** of security monitoring…

QUALYS®

Instead of **Reports,** Qualys is **pioneering** a fundamental shift – to **Events**…

QUALYS®

We call it:

Continuous Security

A **continuous** stream of **all** the **changes** in your environment and **security** posture.

QUALYS®

Qualys is **far more** than just vulnerability data.

1+ Billion Scans Per Year

Vulnerabilities

Open Ports

Installed Software

Web Application Firewall Events

Malware

Web App Bugs

Compliance and Configuration

SSL Certificates

QUALYS®

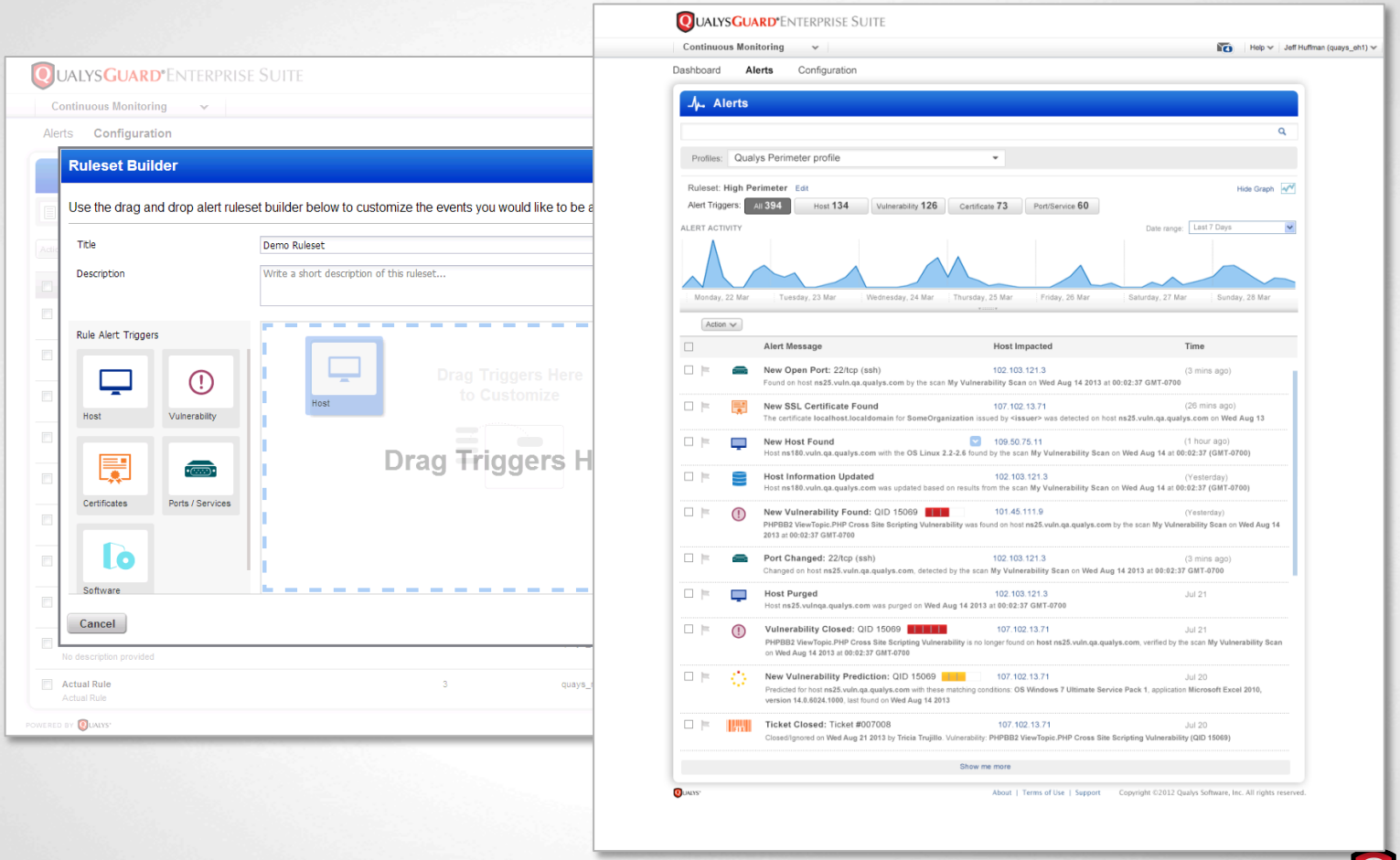
401,856,255,180

(about 400+ billion events per year)

QUALYS®

Very **powerful** filtering engine with a very **simple** interface.

QUALYS®


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Alerts
Configuration
Ruleset Builder
Use the drag and drop alert ruleset builder below to customize the events you would like to be a
Title
Demo Ruleset
Description
Write a short description of this ruleset...
Rule Alert Triggers
Host
Vulnerability
Certificates
Ports / Services
Software
Drag Triggers Here to Customize
Drag Triggers H
Cancel
No description provided
Actual Rule
Actual Rule
QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Jeff Huffman (quays_eh1)
Dashboard
Alerts
Configuration
Alerts
Profiles:
Qualys Perimeter profile
Ruleset: High Perimeter
Edit
Hide Graph
Alert Triggers:
All 394
Host 134
Vulnerability 126
Certificate 73
Port/Service 60
ALERT ACTIVITY
Date range:
Last 7 Days
Monday, 22 Mar
Tuesday, 23 Mar
Wednesday, 24 Mar
Thursday, 25 Mar
Friday, 26 Mar
Saturday, 27 Mar
Sunday, 28 Mar
Action
Alert Message
Host Impacted
Time
New Open Port: 22/tcp (ssh)
102.103.121.3
(3 mins ago)
New SSL Certificate Found
107.102.13.71
(26 mins ago)
New Host Found
109.50.75.11
(1 hour ago)
Host Information Updated
102.103.121.3
(Yesterday)
New Vulnerability Found: QID 15069
101.45.111.9
(Yesterday)
Port Changed: 22/tcp (ssh)
102.103.121.3
(3 mins ago)
Host Purged
102.103.121.3
Jul 21
Vulnerability Closed: QID 15069
107.102.13.71
Jul 21
New Vulnerability Prediction: QID 15069
107.102.13.71
Jul 20
Ticket Closed: Ticket #007008
107.102.13.71
Jul 20
Show me more
About | Terms of Use | Support
Copyright ©2012 Qualys Software, Inc. All rights reserved.

QUALYS®

Demo!

(may the odds be ever in my favor)

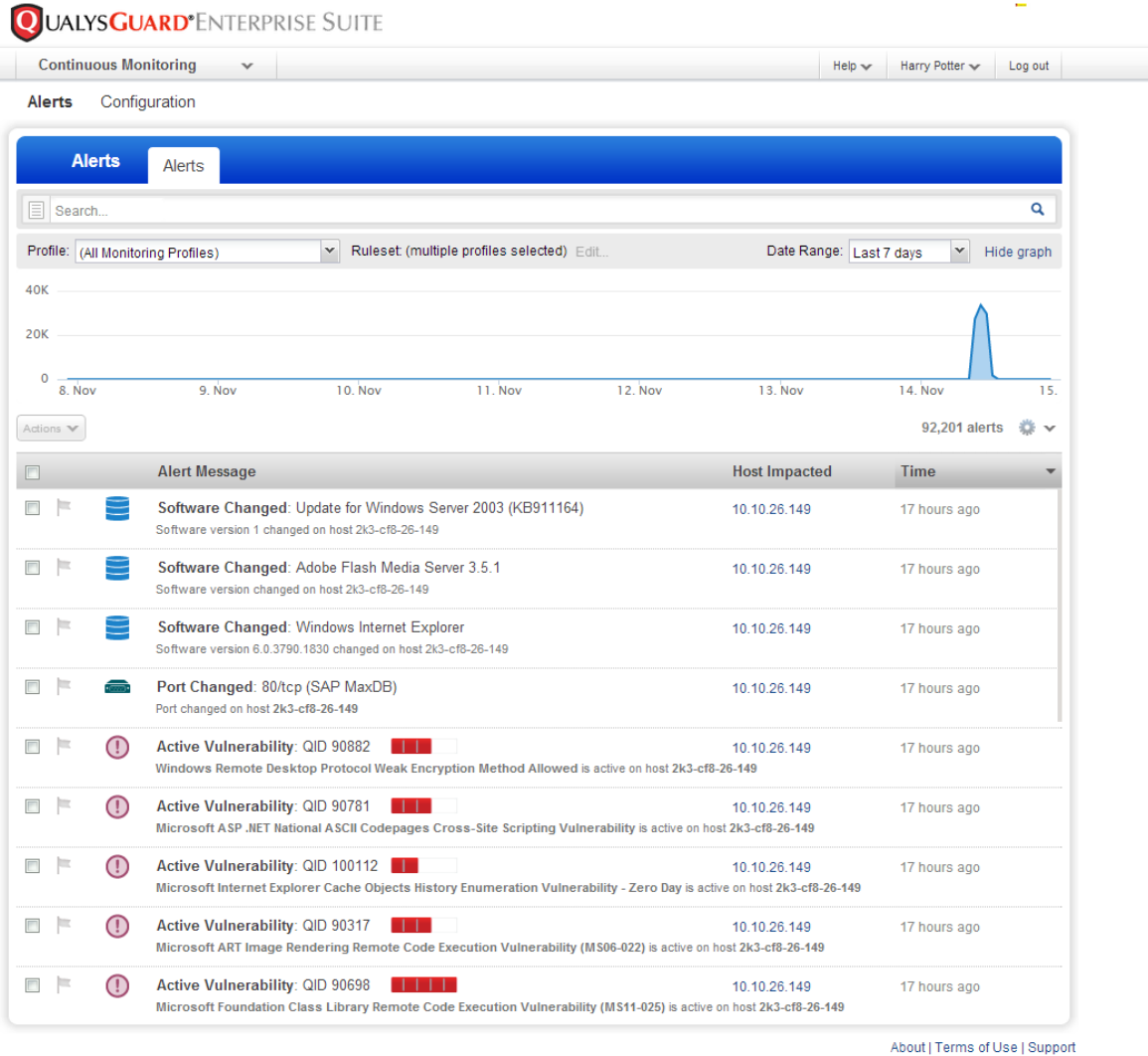
QUALYS®

QUALYS®

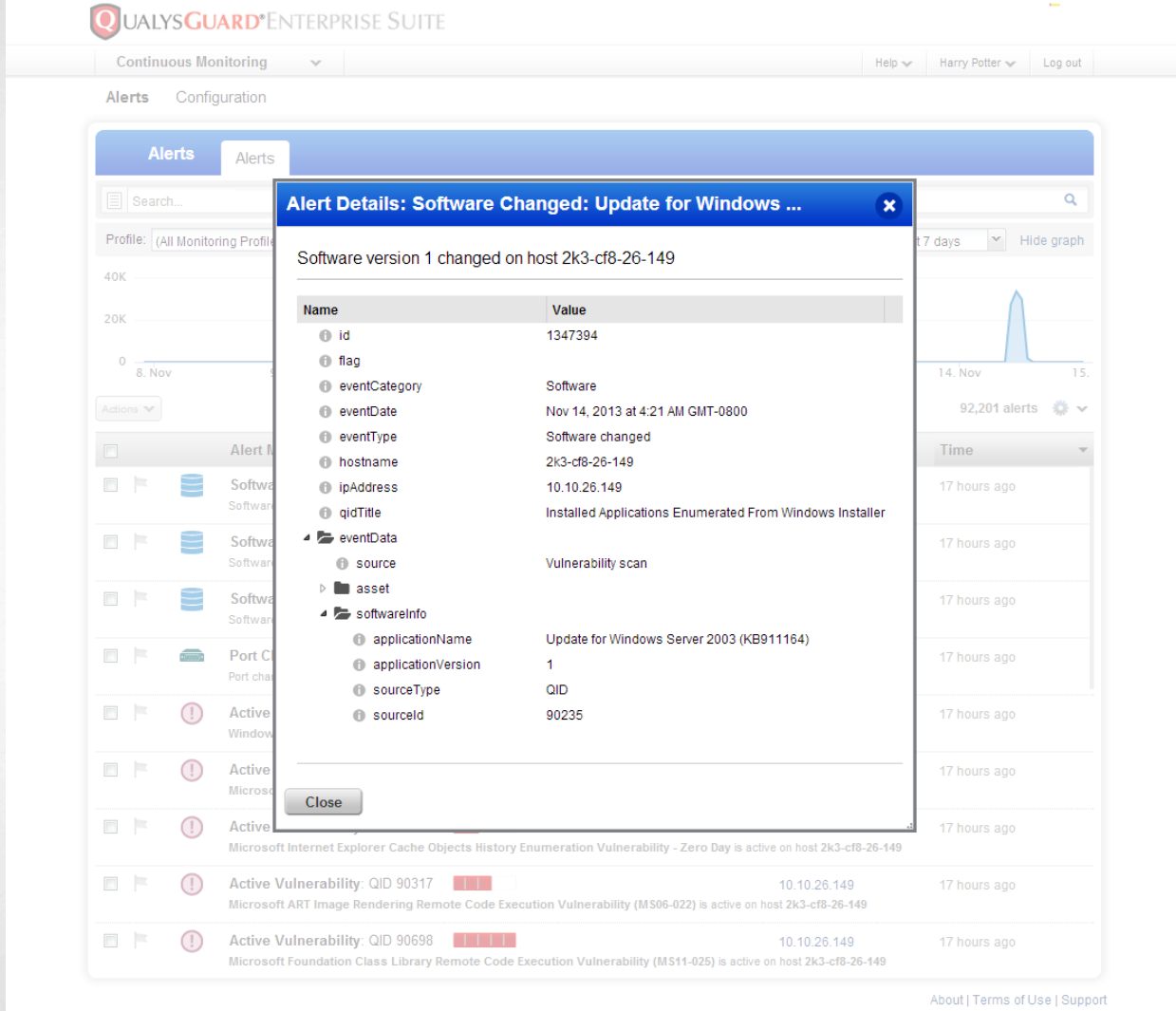
CONTINUOUS SECURITY

Thank You

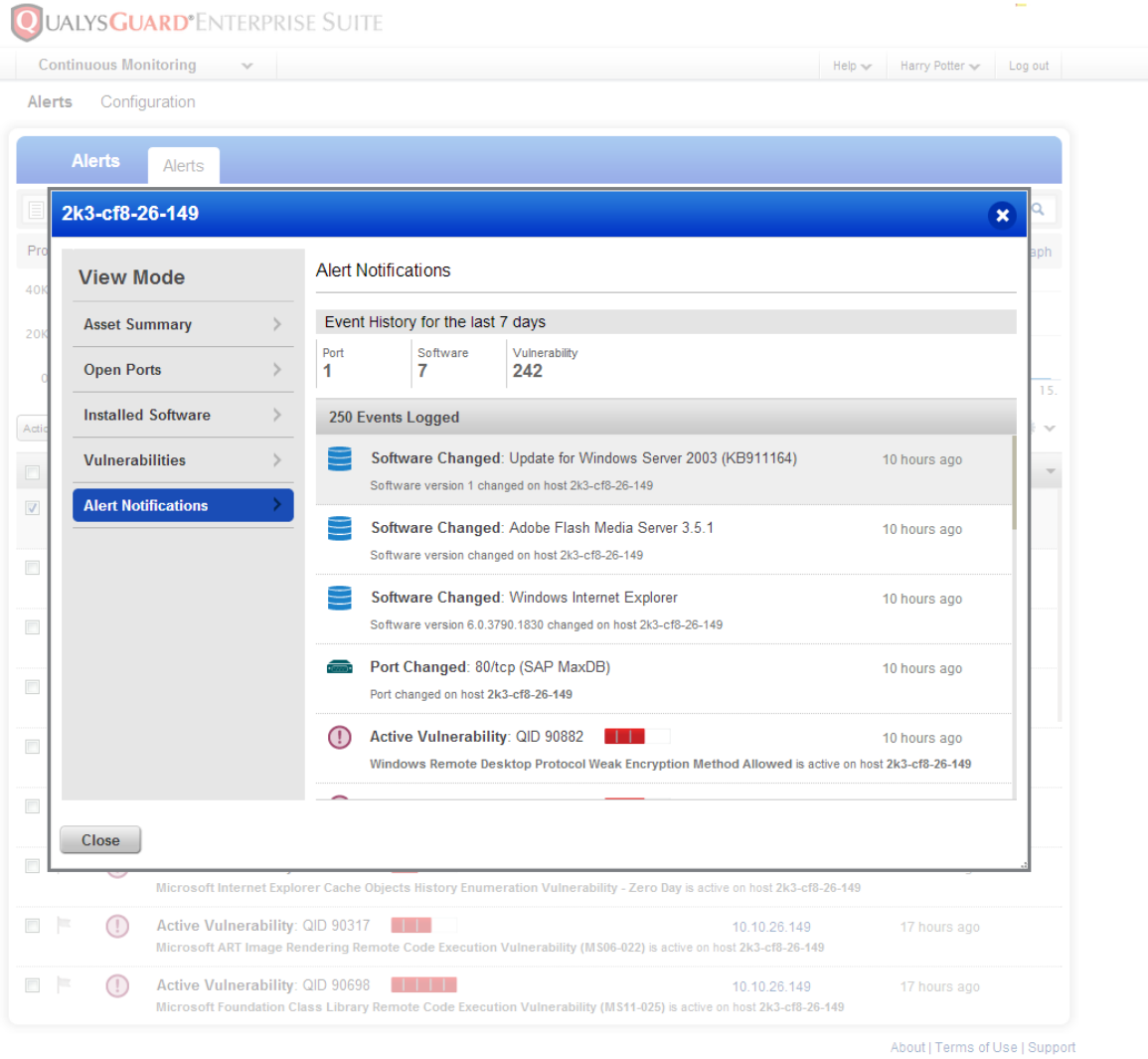
smolloy@qualys.com


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
Search...
Profile: (All Monitoring Profiles)
Ruleset: (multiple profiles selected) Edit...
Date Range: Last 7 days
Hide graph
40K
20K
0
8. Nov
9. Nov
10. Nov
11. Nov
12. Nov
13. Nov
14. Nov
15.
Actions
92,201 alerts
Alert Message
Host Impacted
Time
Software Changed: Update for Windows Server 2003 (KB911164)
Software version 1 changed on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Software Changed: Adobe Flash Media Server 3.5.1
Software version changed on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Software Changed: Windows Internet Explorer
Software version 6.0.3790.1830 changed on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Port Changed: 80/tcp (SAP MaxDB)
Port changed on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Active Vulnerability: QID 90882
Windows Remote Desktop Protocol Weak Encryption Method Allowed is active on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Active Vulnerability: QID 90781
Microsoft ASP .NET National ASCII Codepages Cross-Site Scripting Vulnerability is active on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Active Vulnerability: QID 100112
Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day is active on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Active Vulnerability: QID 90317
Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022) is active on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
Active Vulnerability: QID 90698
Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) is active on host 2k3-cf8-26-149
10.10.26.149
17 hours ago
About | Terms of Use | Support

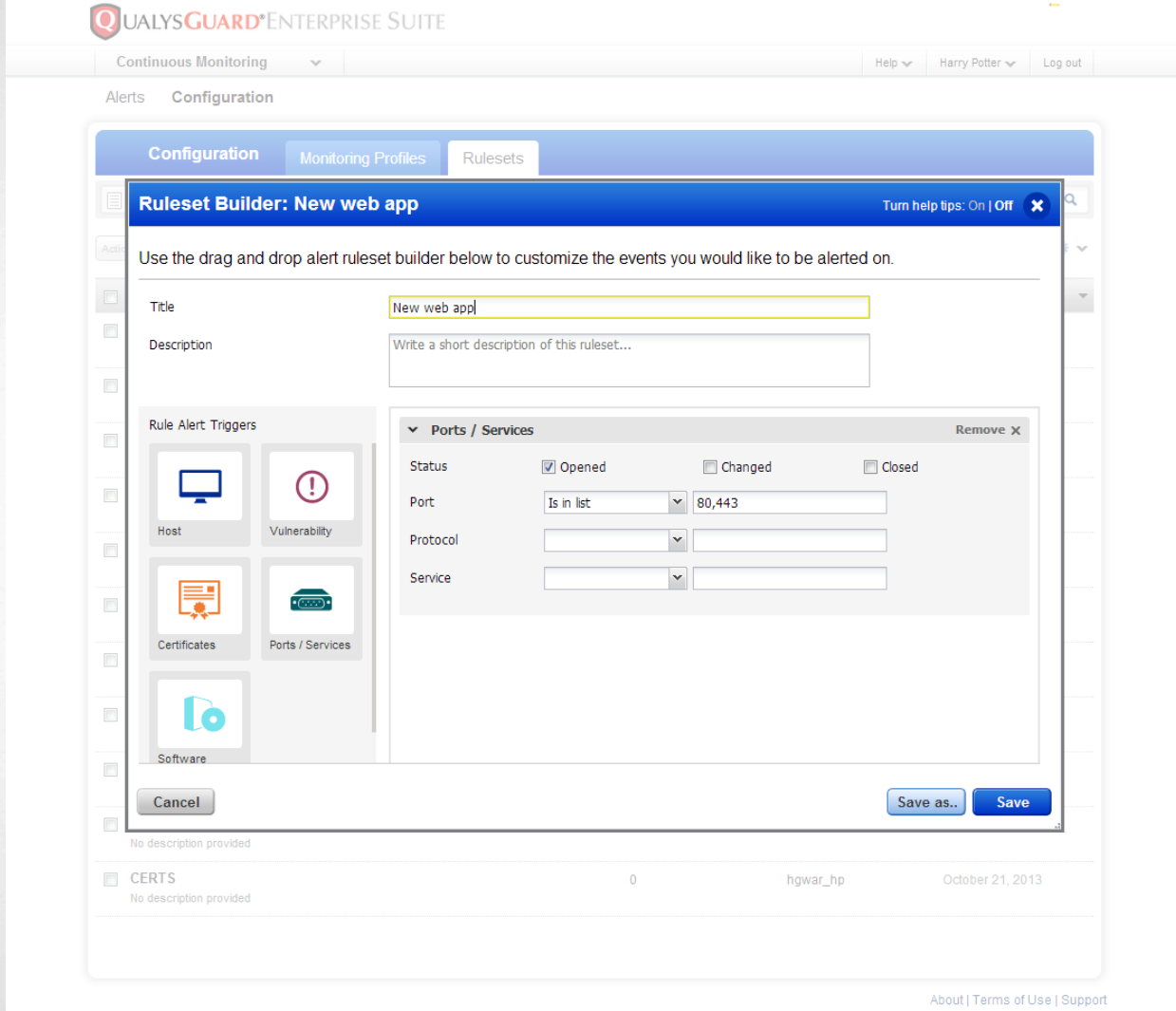
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
Search...
Profile:
(All Monitoring Profile
7 days
Hide graph
40K
20K
0
8. Nov
14. Nov
15.
Actions
92,201 alerts
Time
17 hours ago
Alert Details: Software Changed: Update for Windows ...
Software version 1 changed on host 2k3-cf8-26-149
Name
Value
id
1347394
flag
eventCategory
Software
eventDate
Nov 14, 2013 at 4:21 AM GMT-0800
eventType
Software changed
hostname
2k3-cf8-26-149
ipAddress
10.10.26.149
qidTitle
Installed Applications Enumerated From Windows Installer
eventData
source
Vulnerability scan
asset
softwareInfo
applicationName
Update for Windows Server 2003 (KB911164)
applicationVersion
1
sourceType
QID
sourceId
90235
Close
Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day is active on host 2k3-cf8-26-149
Active Vulnerability: QID 90317
10.10.26.149
Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022) is active on host 2k3-cf8-26-149
Active Vulnerability: QID 90698
10.10.26.149
Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) is active on host 2k3-cf8-26-149
About | Terms of Use | Support

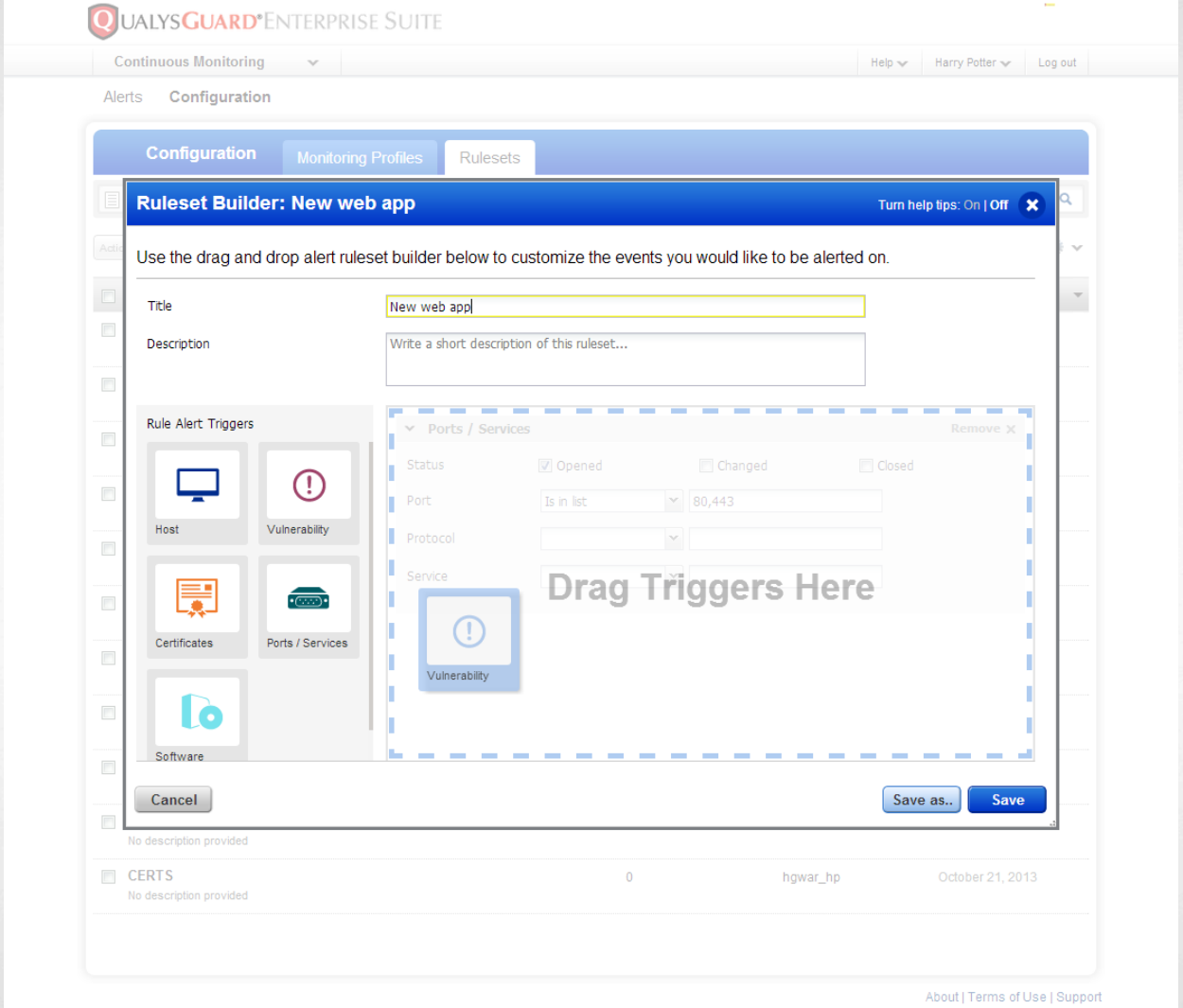
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
2k3-cf8-26-149
View Mode
Asset Summary
Open Ports
Installed Software
Vulnerabilities
Alert Notifications
Alert Notifications
Event History for the last 7 days
Port
1
Software
7
Vulnerability
242
250 Events Logged
Software Changed: Update for Windows Server 2003 (KB911164)
10 hours ago
Software version 1 changed on host 2k3-cf8-26-149
Software Changed: Adobe Flash Media Server 3.5.1
10 hours ago
Software version changed on host 2k3-cf8-26-149
Software Changed: Windows Internet Explorer
10 hours ago
Software version 6.0.3790.1830 changed on host 2k3-cf8-26-149
Port Changed: 80/tcp (SAP MaxDB)
10 hours ago
Port changed on host 2k3-cf8-26-149
Active Vulnerability: QID 90882
10 hours ago
Windows Remote Desktop Protocol Weak Encryption Method Allowed is active on host 2k3-cf8-26-149
Close
Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day is active on host 2k3-cf8-26-149
Active Vulnerability: QID 90317
10.10.26.149
17 hours ago
Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022) is active on host 2k3-cf8-26-149
Active Vulnerability: QID 90698
10.10.26.149
17 hours ago
Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) is active on host 2k3-cf8-26-149
About | Terms of Use | Support

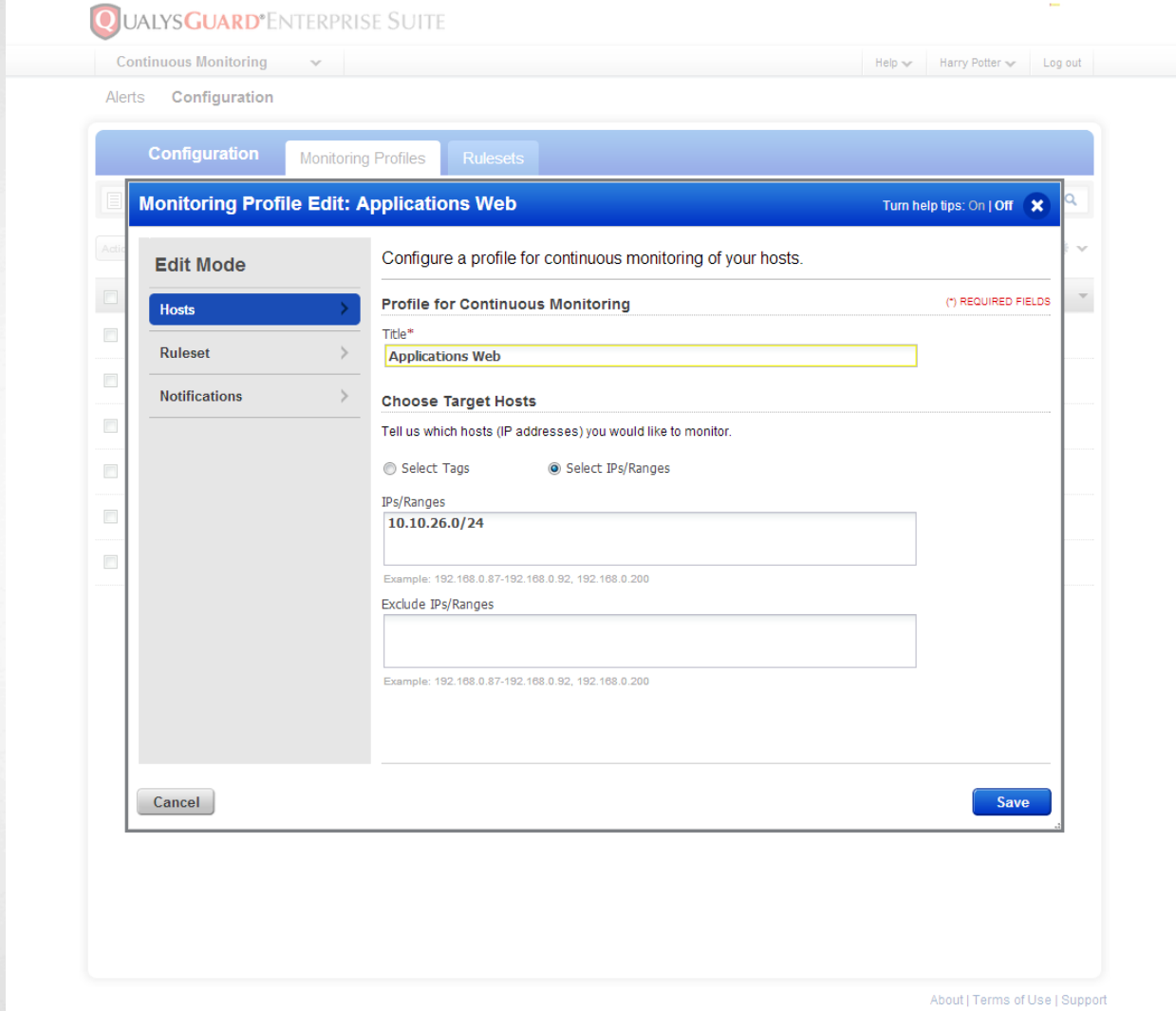
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Configuration
Monitoring Profiles
Rulesets
Ruleset Builder: New web app
Turn help tips: On | Off
Use the drag and drop alert ruleset builder below to customize the events you would like to be alerted on.
Title
New web app
Description
Write a short description of this ruleset...
Rule Alert Triggers
Host
Vulnerability
Certificates
Ports / Services
Software
Ports / Services
Remove
Status
Opened
Changed
Closed
Port
Is in list
80,443
Protocol
Service
Cancel
Save as..
Save
No description provided
CERTS
No description provided
0
hgwar_hp
October 21, 2013
About | Terms of Use | Support

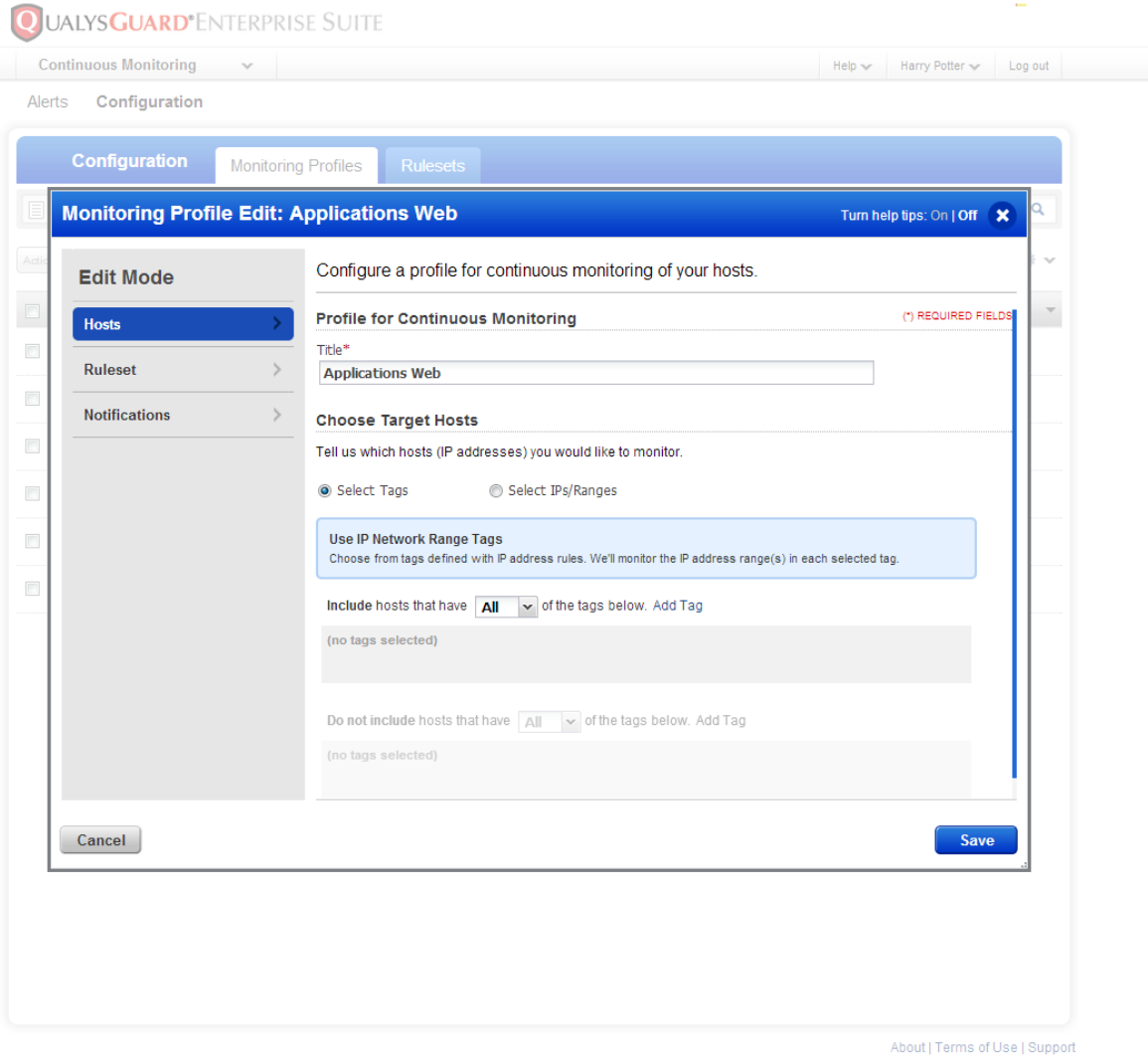
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Configuration
Monitoring Profiles
Rulesets
Ruleset Builder: New web app
Turn help tips: On | Off
Use the drag and drop alert ruleset builder below to customize the events you would like to be alerted on.
Title
New web app
Description
Write a short description of this ruleset...
Rule Alert Triggers
Host
Vulnerability
Certificates
Ports / Services
Software
Ports / Services
Remove
Status
Opened
Changed
Closed
Port
Is in list
80,443
Protocol
Service
Drag Triggers Here
Vulnerability
Cancel
Save as..
Save
No description provided
CERTS
No description provided
0
hgwar_hp
October 21, 2013
About | Terms of Use | Support

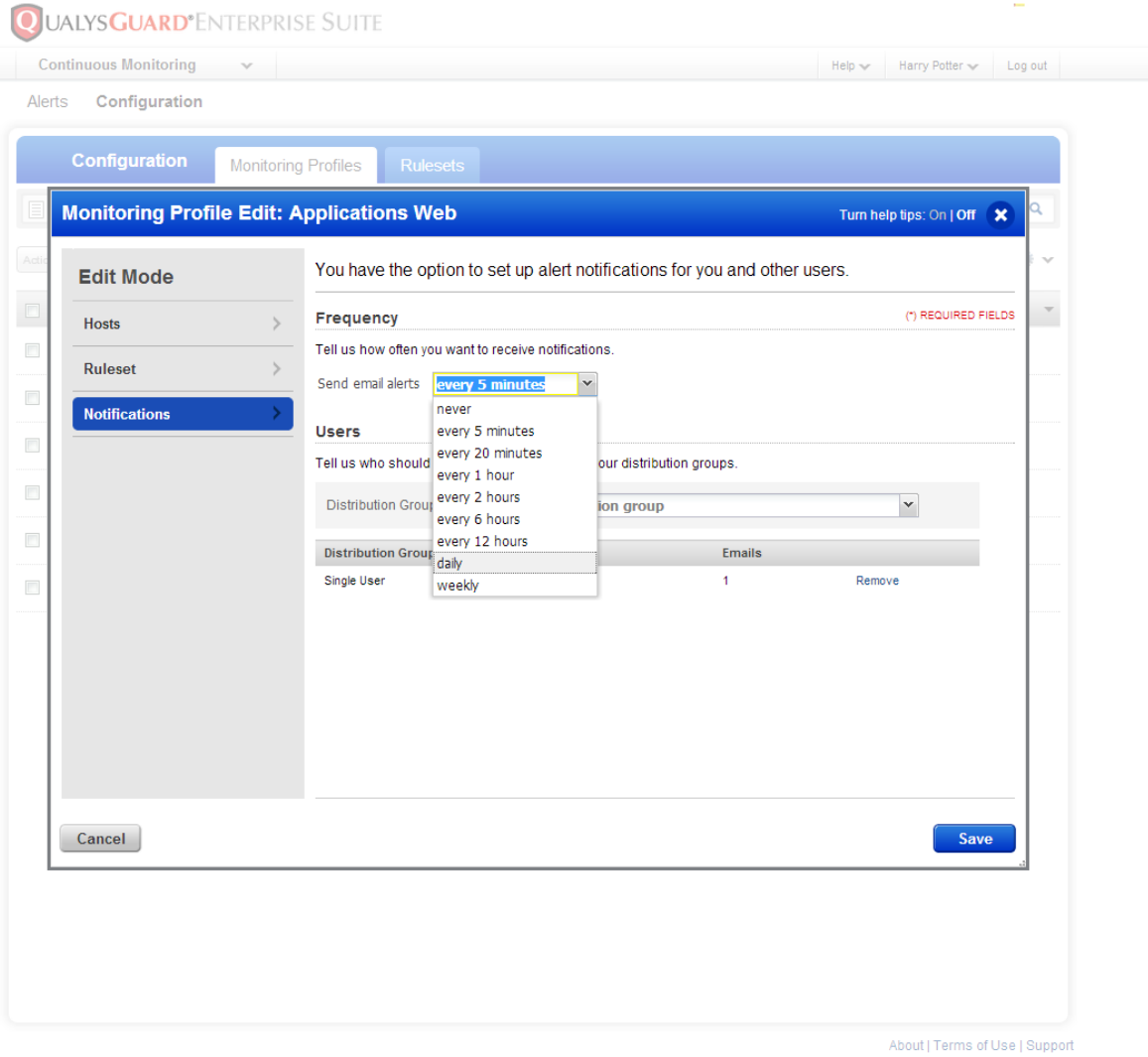
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Configuration
Monitoring Profiles
Rulesets
Monitoring Profile Edit: Applications Web
Turn help tips: On | Off
Edit Mode
Hosts
Ruleset
Notifications
Configure a profile for continuous monitoring of your hosts.
Profile for Continuous Monitoring
(*) REQUIRED FIELDS
Title*
Applications Web
Choose Target Hosts
Tell us which hosts (IP addresses) you would like to monitor.
Select Tags
Select IPs/Ranges
IPs/Ranges
10.10.26.0/24
Example: 192.168.0.87-192.168.0.92, 192.168.0.200
Exclude IPs/Ranges
Example: 192.168.0.87-192.168.0.92, 192.168.0.200
Cancel
Save
About | Terms of Use | Support

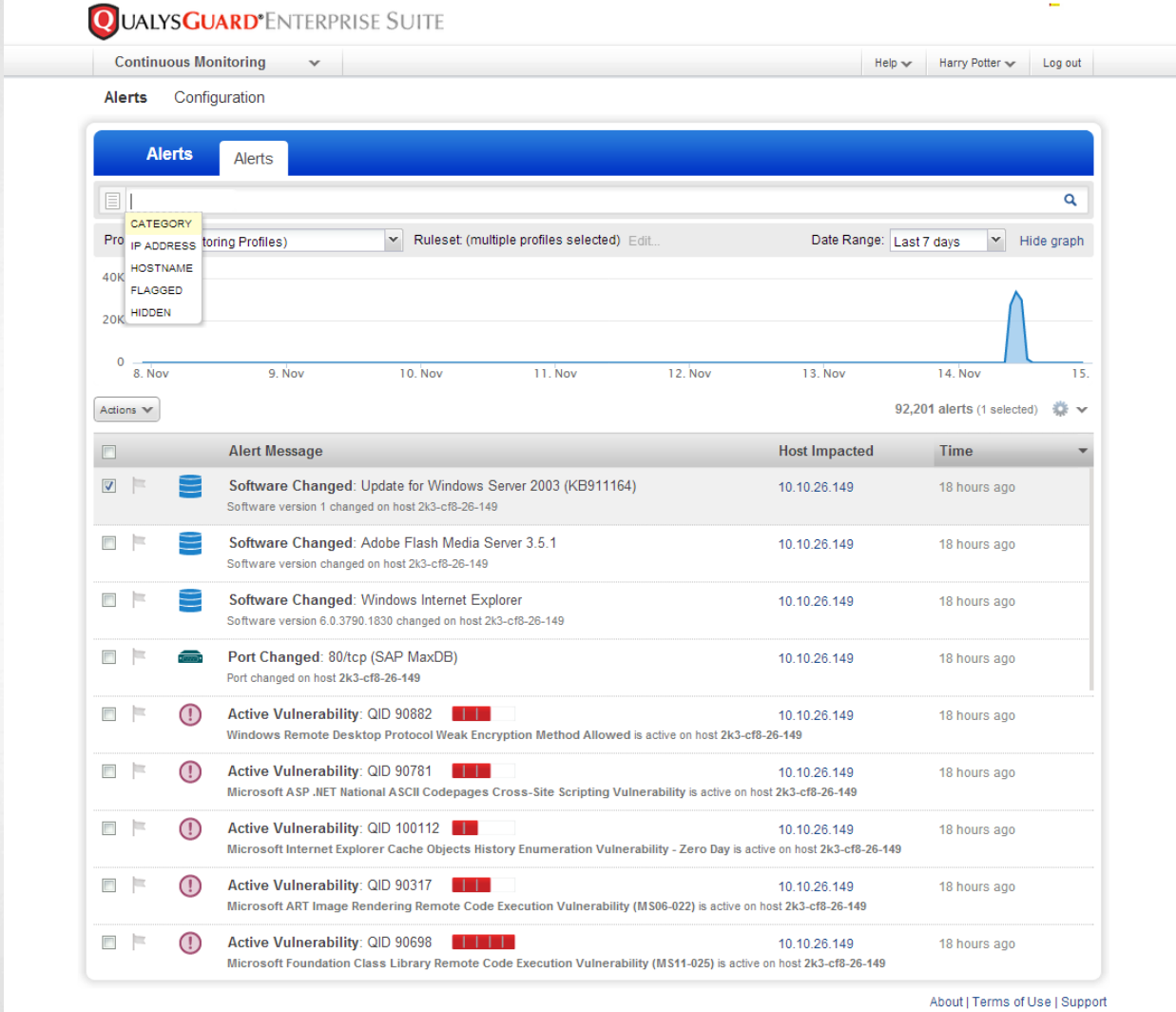
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Configuration
Monitoring Profiles
Rulesets
Monitoring Profile Edit: Applications Web
Turn help tips: On | Off
Edit Mode
Hosts
Ruleset
Notifications
Configure a profile for continuous monitoring of your hosts.
Profile for Continuous Monitoring
(*) REQUIRED FIELDS
Title*
Applications Web
Choose Target Hosts
Tell us which hosts (IP addresses) you would like to monitor.
Select Tags
Select IPs/Ranges
Use IP Network Range Tags
Choose from tags defined with IP address rules. We'll monitor the IP address range(s) in each selected tag.
Include hosts that have All of the tags below. Add Tag
(no tags selected)
Do not include hosts that have All of the tags below. Add Tag
(no tags selected)
Cancel
Save
About | Terms of Use | Support

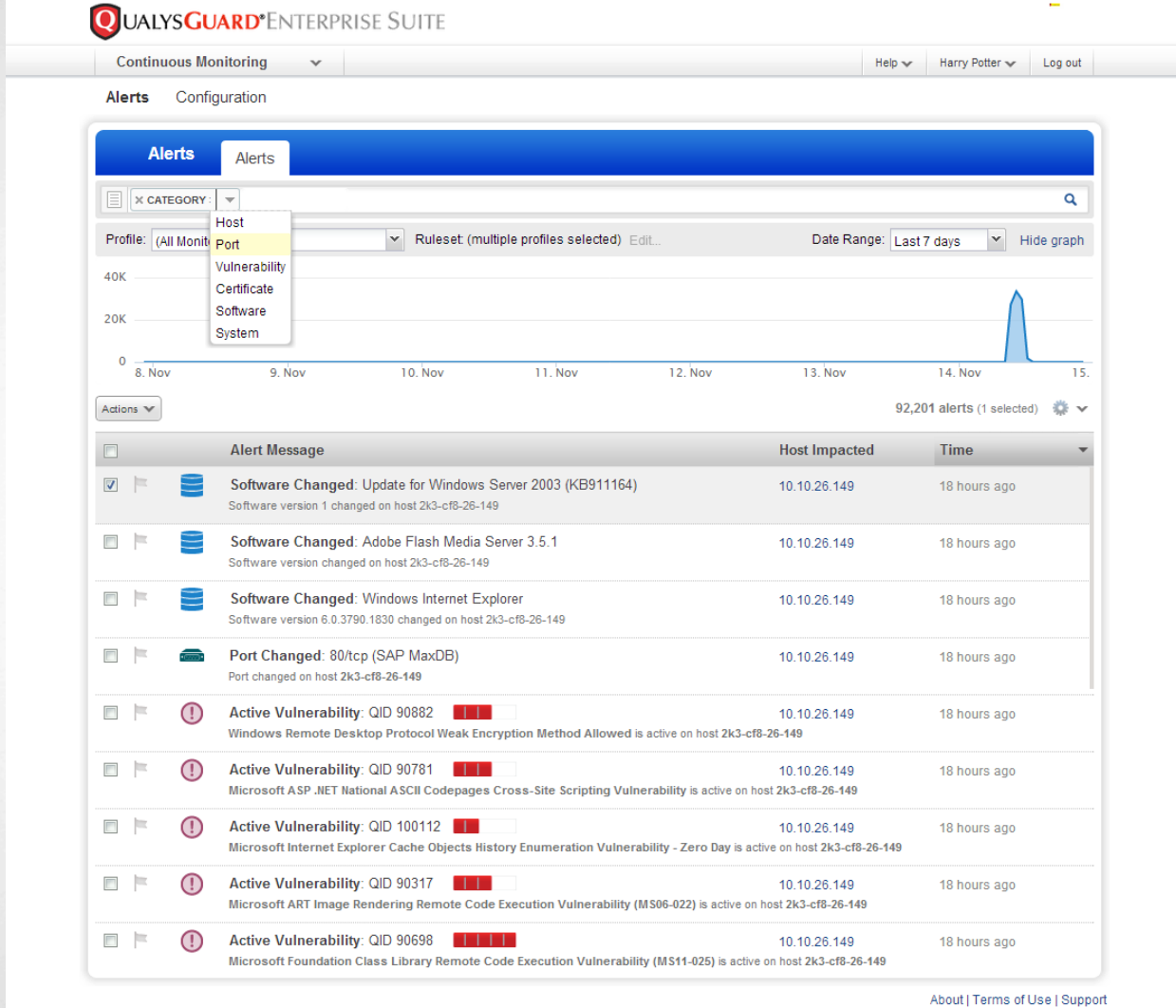
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Configuration
Monitoring Profiles
Rulesets
Monitoring Profile Edit: Applications Web
Turn help tips: On | Off
Edit Mode
Hosts
Ruleset
Notifications
You have the option to set up alert notifications for you and other users.
Frequency
(*) REQUIRED FIELDS
Tell us how often you want to receive notifications.
Send email alerts
every 5 minutes
never
every 5 minutes
every 20 minutes
every 1 hour
every 2 hours
every 6 hours
every 12 hours
daily
weekly
Users
Tell us who should
our distribution groups.
Distribution Group
ion group
Distribution Group
Emails
Single User
1
Remove
Cancel
Save
About | Terms of Use | Support

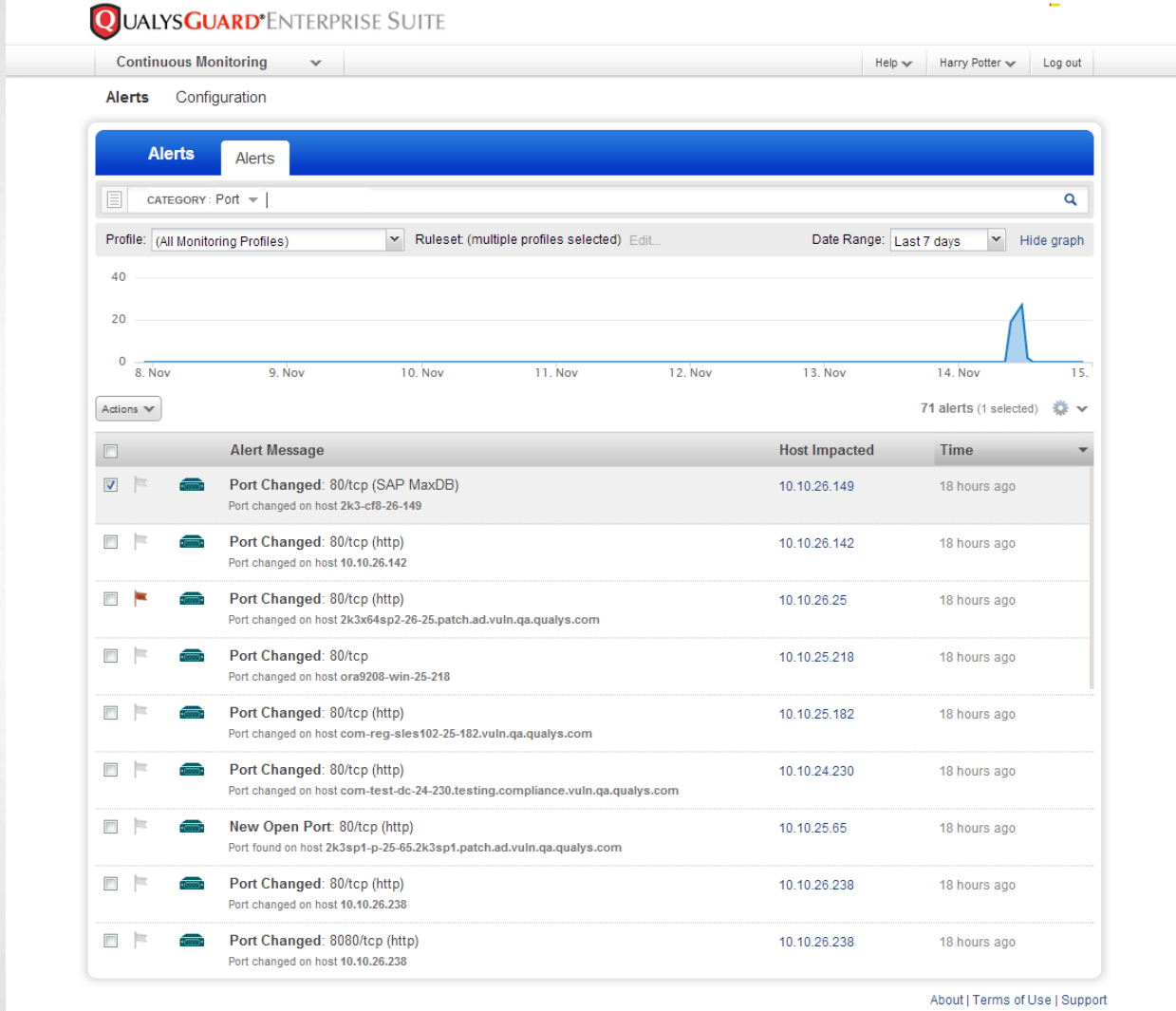
QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
CATEGORY
IP ADDRESS
HOSTNAME
FLAGGED
HIDDEN
Ruleset: (multiple profiles selected)
Edit...
Date Range:
Last 7 days
Hide graph
40K
20K
0
8. Nov
9. Nov
10. Nov
11. Nov
12. Nov
13. Nov
14. Nov
Actions
92,201 alerts (1 selected)
Alert Message
Host Impacted
Time
Software Changed: Update for Windows Server 2003 (KB911164)
Software version 1 changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Software Changed: Adobe Flash Media Server 3.5.1
Software version changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Software Changed: Windows Internet Explorer
Software version 6.0.3790.1830 changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Port Changed: 80/tcp (SAP MaxDB)
Port changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90882
Windows Remote Desktop Protocol Weak Encryption Method Allowed is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90781
Microsoft ASP .NET National ASCII Codepages Cross-Site Scripting Vulnerability is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 100112
Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90317
Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022) is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90698
Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
About | Terms of Use | Support

QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
CATEGORY
Host
Port
Vulnerability
Certificate
Software
System
Profile:
Ruleset: (multiple profiles selected)
Edit...
Date Range:
Last 7 days
Hide graph
40K
20K
0
8. Nov
9. Nov
10. Nov
11. Nov
12. Nov
13. Nov
14. Nov
15.
Actions
92,201 alerts (1 selected)
Alert Message
Host Impacted
Time
Software Changed: Update for Windows Server 2003 (KB911164)
Software version 1 changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Software Changed: Adobe Flash Media Server 3.5.1
Software version changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Software Changed: Windows Internet Explorer
Software version 6.0.3790.1830 changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Port Changed: 80/tcp (SAP MaxDB)
Port changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90882
Windows Remote Desktop Protocol Weak Encryption Method Allowed is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90781
Microsoft ASP .NET National ASCII Codepages Cross-Site Scripting Vulnerability is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 100112
Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90317
Microsoft ART Image Rendering Remote Code Execution Vulnerability (MS06-022) is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Active Vulnerability: QID 90698
Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) is active on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
About | Terms of Use | Support

QUALYS


QUALYSGUARD ENTERPRISE SUITE
Continuous Monitoring
Help
Harry Potter
Log out
Alerts
Configuration
Alerts
Alerts
CATEGORY : Port
Profile: (All Monitoring Profiles)
Ruleset: (multiple profiles selected) Edit...
Date Range: Last 7 days
Hide graph
40
20
0
8. Nov
9. Nov
10. Nov
11. Nov
12. Nov
13. Nov
14. Nov
15.
Actions
71 alerts (1 selected)
Alert Message
Host Impacted
Time
Port Changed: 80/tcp (SAP MaxDB)
Port changed on host 2k3-cf8-26-149
10.10.26.149
18 hours ago
Port Changed: 80/tcp (http)
Port changed on host 10.10.26.142
10.10.26.142
18 hours ago
Port Changed: 80/tcp (http)
Port changed on host 2k3x64sp2-26-25.patch.ad.vuln.qa.qualys.com
10.10.26.25
18 hours ago
Port Changed: 80/tcp
Port changed on host ora9208-win-25-218
10.10.25.218
18 hours ago
Port Changed: 80/tcp (http)
Port changed on host com-reg-sles102-25-182.vuln.qa.qualys.com
10.10.25.182
18 hours ago
Port Changed: 80/tcp (http)
Port changed on host com-test-dc-24-230.testing.compliance.vuln.qa.qualys.com
10.10.24.230
18 hours ago
New Open Port: 80/tcp (http)
Port found on host 2k3sp1-p-25-65.2k3sp1.patch.ad.vuln.qa.qualys.com
10.10.25.65
18 hours ago
Port Changed: 80/tcp (http)
Port changed on host 10.10.26.238
10.10.26.238
18 hours ago
Port Changed: 8080/tcp (http)
Port changed on host 10.10.26.238
10.10.26.238
18 hours ago
About | Terms of Use | Support

QUALYS